RATACA: ROBUST AND AUTHENTIC TECHNIQUE AGAINST COLLUSION ATTACK

Jyoti Chaudhary[1], Sonam Kataria[2]

[1,]Assistant Professor, [2]Student, CSE/MDU (India)

ABSTRACT

The main work of any sensor network is to transfer the accurate data to the destination. The collusion attack biased the nodes to change the reading of the sensor nodes. It leads to inaccurate readings. This paper describes a technique that handles the collusion attack by discarding the biased nodes. The technique determines the reliability factor of each node and discards the less reliable nodes to increase the accuracy of the readings. The analysis is done by calculating the MSE. The decrease in the MSE in biased network as well as in unbiased network shows the significance of the technique.

Keywords: Absolute error, Collision Attack, Weight, WSN, MSE.

I. INTRODUCTION

Wireless sensor network consists of tiny sensor nodes that are used to collect the data. The collected data by the sensor nodes is transferred to the sink node which forwards it to the server via internet. The accuracy of the collected data is the main issue of concern for the users. There exist several attacks in the WSN which leads to change in the reading of the sensor data. One of them is the collusion attack.

In the collusion attack the sensor nodes are biased to generate the inaccurate readings. The initial biasing of the nodes leads to the inaccurate readings. The biasing can be due hardware fault or can be done intentionally. For example, if any company deployed 400 sensors in different area to analyze the pressure. Few sensors are initially biased to -50 reading then the actual reading of 200 will be displayed as 150 which lead to the inaccurate data. The average pressure measured due to this will be lower than the actual pressure. The collusion attack must be handled properly as accuracy of the data is required. The traditional techniques take the average of all the readings to get the calculated value. But the error in such technique seems to be large. So this paper describes filtering based techniques to handle the collusion attack. The rest paper is divided in four sections, first section describes related work, second section describes the existing filtering technique. The third section describes the present algorithm to handle the collusion attack. Then the final section describes the results of the simulation.

II. RELATED WORK

Pardeep Kumar et. [1] proposesa efficient and robust scheme for user authentication in wireless sensor networks. The scheme is based on anonymity, secure session key establishment and mutual authentication concept. Dong Jiao, et. al. [2] proposed a modified scheme for the key-distribution. The scheme is based on secret sharing and provides, long lifespan and lower communication overhead .Sankardas Roy [3] presents an algorithm for the secure communication even in the presence of attack. Their algorithm computes the true aggregate by filtering out the contributions of compromised nodes in the aggregation hierarchy. Mohsen Rezvaniet. al. [4] discussed various existing filtering techniques to handle collusion attack and improved the existing filtering techniques by using an initial approximation. It leads to more accurate and faster converging.

III. FILTERING TECHNIQUE

In the collusion attack the unintended authority generates bias that deviates the senor reading from the original value. It may lead to the change reading as compared to the original reading available to the user. The filtering technique gives the original value of the reading even after the biasing of the senor node. The steps of the filtering are given below:

```
1.  Initiate network with n sensors with m reading each.
2.  X= reading for the sensors. (For simulation reading are generated randomly using randi(n,m))
3.  Temp=0;
4.  W(temp)=1 where W(0) is the initial weight vector.
5.  R(temp)=0.
6.  R(temp+1)=mean(X)
7.  While R(temp)!=R(temp+1)
8.  D(i)=(X(i)-R(temp+1))/m
9.  R(temp+1)=X.W(temp)/sum(W)
10. Update W(temp+1)=g(d)
11. Temp=temp+1
12. End
13. Note the reading
```

The above algorithm results in the accurate reading even after biasing. The accuracy can be improved discussed in next section.

IV. FILTERING & DISCARDING TECHNIQUE

In the existing technique collusion attack is handled by using the iterative filtering of data. The defined procedure repeats number of times and filter the data to get the accurate reading but the existing technique enable to handle the adversary attack. It means if the compromised nodes are sharing data with any third party that deviates the data of the nodes. Then the data sharing continues even after the use of the existing iterative algorithm. In this work the node with biasing is detected and readjusted to zero bias. If in next few reading the problem continues then the node is discarded. The process can be explained by the following algorithm:

4.1 Filtering & Discarding Algorithm

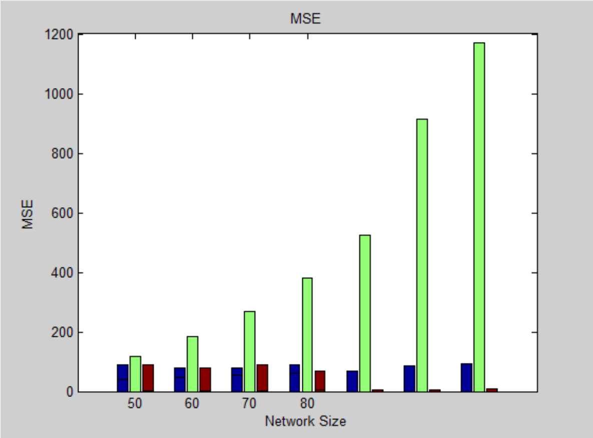
```
1.  Initiate network with n sensors with m reading each.
2.  Process_rep=10;
3.  Status(1:n)=0;
4.  For i=1:process_rep
```

```
5.  X= reading for the sensors. (For simulation reading are generated randomly using randi(n,m))
6.  Temp=0;
7.  W(temp)=1 where W(0) is the initial weight vector.
8.  R(temp)=0.
9.  R(temp+1)=mean(X)
10. While R(temp)!=R(temp+1)
11. D(i)=(X(i)-R(temp+1))/m
12. R(temp+1)=X.W(temp)/sum(W)
13. Update W(temp+1)=g(d)
14. Temp=temp+1
15. End
16. Note the reading
17. B_sensor=Min(r)
18. Set baising of B_Sensor to 0.
19. If status(B_sensor)==0
20. Status(B_sensor)=1
21. Else
22. Discard the node
23. Remove the X(B_sensor).
24. end
25. end
```

The steps of the algorithm explain the process briefly. The above process can be implemented using MATLAB discussed in next section.

V. RESULTS & DISCUSSION

The MATLAB doesn’t contain any toolbox for the WSN so the implementation is done by using the script file generated using the editor window. Three parameters i.e. MSE, variance and the absolute error is calculated to analyze the results. The MSE stands for mean square error and can be calculated as mean ((calculated_reading-actual_reading).^2). The square root of the MSE is known as the variance i.e. sqrt (mean ((calculated_reading-actual_reading).^2)). The absolute error is given as mean ((calculated_reading-actual_reading)). The absolute error shows the mean of the change in the reading but the negative values can balance some positive values. So the deviation and the variance are evaluated to know the exact deviation. But the absolute error will give the exact error to be handled. The analysis is done on the traditional techniques that performs simple averaging to get the results and the filtering techniques described in previous sections.



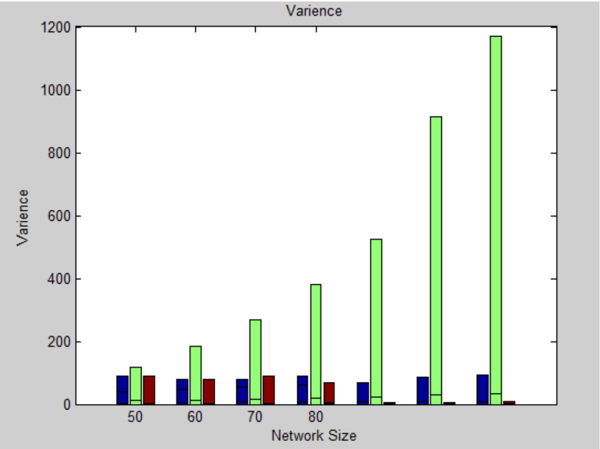
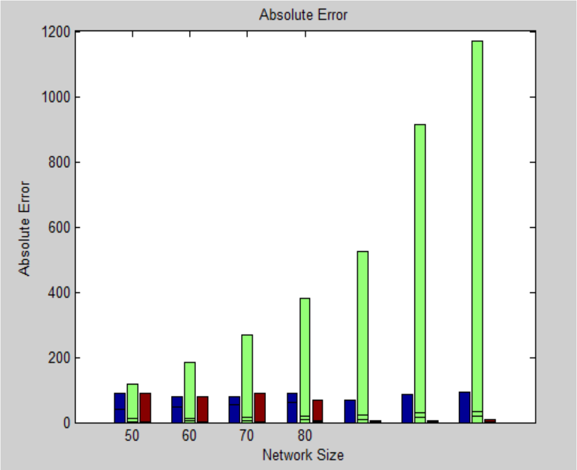


Fig.1: Mean Square Error without Biasing

Fig.2: Variance without Biasing



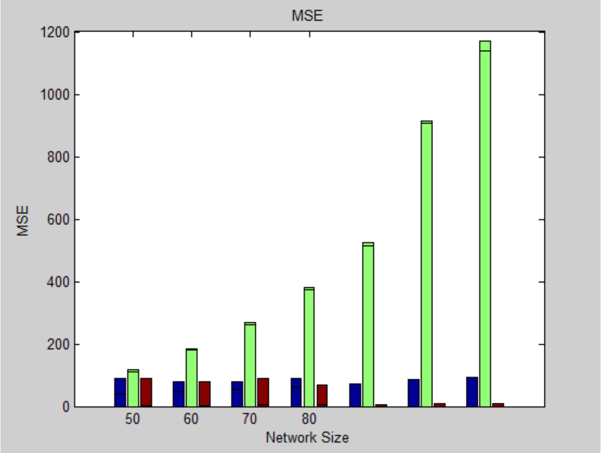
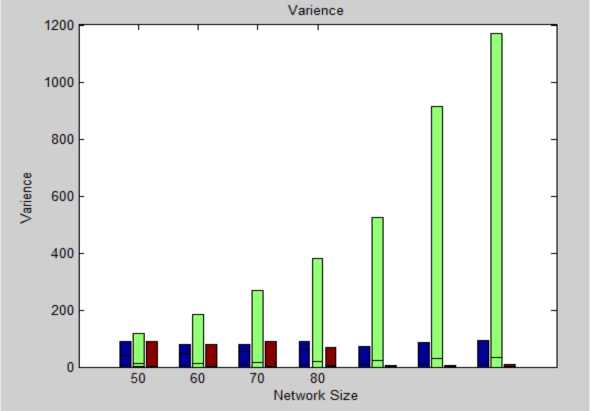


Fig.3: Absolute Error without Biasing

Fig.4: Mean Square Error with Biasing



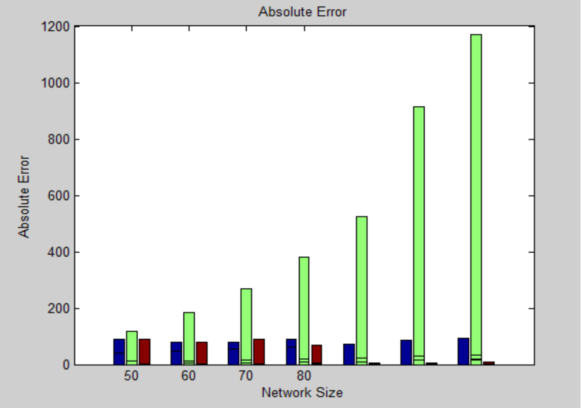


Fig.5: Variance with Biasing

Fig.6: Absolute Error without Biasing

VI. CONCLUSION

This paper describes the collusion attack and a technique to handle the collusion attack. The existing filtering techniques are less accurate so a discarding process is added to the filtering technique to improve the performance. The work is implemented using the MATLAB. The result analysis shows that the described technique is effective as MSE get decreased. The absolute error as well as the variance is also decreased. In future the technique can be extended to handle the network layer attacks.

REFERENCES

[1]. Pardeep Kumar 1, Amlan Jyoti Choudhury 1, Mangal Sain 1, Sang-Gon Lee 2,* and Hoon-Jae Lee 2, “RUASN: A Robust User Authentication Framework for Wireless Sensor Network ,”Sensors 2011, 11, 5020-5046; doi:10.3390/s110505020.

[2]. DongJiao,1 MingchuLi,1 YanYu,2 and JinpingOu3, “Self-Healing Key-Distribution Scheme with Collusion Attack Resistance Based on One-Way Key Chains and Secret Sharing in Wireless Sensor Networks,” Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2012, Article ID 821486, 7 pages doi:10.1155/2012/821486.

[3]. Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia, “Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker’s Impact,” IEEE transaction on information forensic and security vol:9 no:4 year2014.

[4]. Mohsen Rezvani, AleksandarIgnjatovic, Elisa Bertino and Sanjay Jha, “Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks,” IEEE transaction on dependable and secure compt., vol. 12, no. 1, Jan/Feb 2015